UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

v.

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a Tollfreedeals.com, and SIP RETAIL d/b/a sipretail.com,

Defendants.

COMPLAINT

Civil Action No.

CV20-473

KORMAN, J.

MANN. M.J.

Plaintiff, the UNITED STATES OF AMERICA, by and through the undersigned attorneys, hereby alleges as follows:

## INTRODUCTION

1. The United States brings this action for a temporary restraining order, preliminary and permanent injunctions, and other equitable relief pursuant to 18 U.S.C. § 1345, in order to enjoin the ongoing commission of criminal wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349. The United States seeks to prevent continuing and substantial injury to the victims of fraud.

2. Since at least 2016 and continuing through the present, Defendants, together with one or more co-conspirators, have used the U.S. telephone system to engage in predatory wire fraud schemes that victimize individuals throughout the United States, including individuals within the Eastern District of New York and significant numbers of elderly and vulnerable victims.

Defendants are VoIP[1] carriers, and their principals, that serve as "gateway carriers,"[2] facilitating the delivery of millions of fraudulent "robocalls"[3] every day from foreign call centers and foreign VoIP carriers to the U.S. telecommunications system and ultimately to phones throughout the United States. The Defendants thus provide foreign fraudsters the means to access the U.S. telephone system, knowingly passing millions of fraudulent robocalls intended to deceive the recipient into: (1) answering or returning the call, and (2) paying money to the perpetrators of the schemes.

3. Through these robocalls, fraudsters operating overseas impersonate government entities and well-known businesses by "spoofing"[4] legitimate phone numbers and sending recorded messages that are transmitted across the internet to telephones throughout the United States. These robocalls purport to be from federal government agencies, elements of foreign governments, and legitimate businesses, conveying alarming messages, such as that the call recipient's social security number or other personal information has been compromised or otherwise connected to criminal activity; the recipient faces imminent arrest; the recipient's assets are being frozen; the recipient's bank and credit accounts have suspect activity; the recipient's benefits are being stopped; the recipient faces imminent deportation; or combinations

---

[1] VoIP stands for voice-over-internet protocol and allows users to place phone calls over a broadband internet connection.

[2] As set forth in greater detail herein, "gateway carriers" are the first in a chain of VoIP carriers located in the United States that facilitate the delivery of foreign VoIP calls to recipients in the United States.

[3] "Robocall" means a call made through an automated process that places large volumes of telephone calls over the internet in order to deliver recorded messages, in contrast to calls placed one at a time by a live person.

[4] The practice of making a false number appear on the recipient's caller ID is known as "spoofing."

of these things—all lies intended to induce potential victims to speak to the fraudsters. When individuals answer the calls or return voicemail messages, the fraudsters offer to "resolve" these legal matters by immediate transfers of funds to settle the purported legal obligation, or to hold the individual's assets only temporarily while the crisis resolves. In reality, the individual is neither under investigation nor in legal jeopardy, and the same threatening robocall was made simultaneously to thousands of other U.S. telephones.

4. Not only do Defendants deliver vast numbers of fraudulent robocalls every day, but they also participate in the fraudulent schemes by providing return-calling services the fraudsters use to establish contact with potential victims. Robocall messages will often provide domestic and toll-free call-back numbers; potential victims who call these numbers connect to the overseas fraudsters, who then try to extort and defraud the potential victims.

5. Defendants profit from these fraudulent robocall schemes by receiving payment from their co-conspirators for the services Defendants provide. Often, these payments consist of victim proceeds, a portion of which is deposited directly into Defendants' accounts in the United States, before the remainder is transmitted to the fraudsters overseas.

6. Since at least 2016 and continuing through the present, as a result of their conduct, Defendants and their co-conspirators have defrauded numerous victims out of millions of dollars, including victims in the Eastern District of New York.

7. For the reasons stated herein, the United States requests injunctive relief pursuant to 18 U.S.C. § 1345 to enjoin Defendants' ongoing schemes to commit wire fraud in violation of 18 U.S.C. § 1343 and conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349.[5]

[5] This case is one of two cases being filed simultaneously in which the United States Department of Justice, for the first time, seeks to enjoin telecommunications companies from participating in robocalling fraud schemes pursuant to 18 U.S.C. § 1345.

## JURISDICTION AND VENUE

8. The Court has subject matter jurisdiction over this action pursuant to 18 U.S.C. § 1345 and 28 U.S.C. §§ 1331 and 1345.

9. Venue lies in this district pursuant to 28 U.S.C. § 1391(b)(2).

## PARTIES

10. Plaintiff is the United States of America.

11. Defendants Nicholas and Natasha Palumbo own and control Ecommerce National, LLC, doing business as TollFreeDeals.com and SIP Retail, LLC, also doing business as SipRetail.com (the "Corporate Defendants"), which the Palumbos utilize in furtherance of the fraudulent robocall schemes. The Palumbos operate the Corporate Defendants from their home in Paradise Valley, Arizona, and on information and belief, the Palumbos operate SIP Retail as an alter ego of Ecommerce. From their home in Paradise Valley, Arizona, the Palumbos operate the Corporate Defendants as fraudulent enterprises.

12. Defendant Ecommerce is a corporation organized and existing under the laws of the State of Arizona. Ecommerce does business as TollFreeDeals.com, and will be referred to throughout this Complaint as TollFreeDeals. TollFreeDeals' principal place of business is located at the Palumbos' home in Paradise Valley, Arizona. Nicholas Palumbo is the Chief Executive Officer of TollFreeDeals and Natasha Palumbo is the Vice President of Business Development.

13. Defendant SIP Retail, LLC, also doing business as SipRetail.com ("SIP Retail"), is a corporation organized and existing under the laws of the State of Arizona. SIP Retail's principal place of business is located at the Palumbos' home in Paradise Valley, Arizona. Natasha Palumbo is the Chief Executive Officer of SIP Retail. SIP Retail provides VoIP carrier services for some of the same customers as TollFreeDeals, including foreign VoIP carriers that

transmit millions of calls every week destined for the phones of residents of the Eastern District of New York.

## OVERVIEW OF THE ROBOCALLING FRAUD SCHEMES

### A. Robocalling Fraud Targeting Individual in the United States

14. The robocalling fraud schemes in which the Defendants are engaged share the same characteristics. Individuals at call centers located abroad, many of which are operating out of India, are bombarding the U.S. telephone system daily with millions of robocalls intended to defraud individuals in the United States. Many of these fraudsters impersonate U.S. government officials, foreign government officials, or well-known American businesses, in order to threaten, defraud, and extort money from robocall recipients. Robocalling technology, which allows fraudsters to send millions of calls per day all transmitting the same pre-recorded, fraudulent message, enables fraudsters to cast a wide net for elderly and vulnerable victims who are particularly susceptible to the threatening messages the fraudsters are sending. Even if only a small percentage of the recipients of a fraudulent call center's robocalls connect with potential victims, the fraudsters can still reap huge profits from their schemes.

15. Foreign fraudsters operate many different scams targeting individuals in the United States, but the Defendants' robocall schemes include the following categories of impersonation scams:

a. *Social Security Administration ("SSA") Imposters*: Defendants transmit recorded messages in which SSA imposters falsely claim that the call recipient's social security number has been used in criminal activity, the recipient's Social Security benefits will be suspended, the recipient has failed to appear before a grand jury and faces imminent arrest, or the recipient's social security number will be

terminated. When a recipient calls back or connects to the fraudster, the fraudster claims to be an SSA employee and typically tells the individual to transfer substantial funds to the SSA for safekeeping until a new social security number can be issued, at which point the funds purportedly will be returned.

b. *Internal Revenue Service ("IRS") Imposters*: Defendants transmit recorded messages in which IRS imposters falsely claim that the call recipient has been implicated in tax fraud, has avoided attempts to enforce criminal laws, has avoided court appearances, or the recipient faces imminent arrest. When a recipient calls back or connects to the fraudster, the fraudster claims to be an IRS or Treasury employee and typically directs the recipient to transfer funds to the IRS to resolve various fictitious tax and legal liabilities, or for safekeeping in order to avoid seizure of assets.

c. *United States Citizenship and Immigration Services ("USCIS") Imposters*: Defendants transmit recorded messages in which USCIS imposters falsely claim that the recipient has failed to fill out immigration forms correctly, the recipient faces imminent arrest or deportation, the recipient's home country has taken formal action against the recipient that may result in deportation, or the recipient has transferred money in a way that will result in deportation. When a recipient calls back or connects to the fraudster, the fraudster claims to be a USCIS employee and typically tells the recipient to pay various fees or fines to avoid immigration consequences.

d. *Tech Support Imposters*: Defendants transmit recorded messages in which fraudsters operating tech support scams impersonate various well-known tech

companies such as Apple or Microsoft, and falsely claim that the recipient has computer security problems that require assistance. When an individual connects with the fraudster, the fraudster instructs the individual to pay for fictitious tech support and computer security services, and to allow the fraudster remote access to the victim's bank accounts.

e. *Loan Approval Scams*: Defendants transmit recorded messages in which fraudsters operating loan approval scams impersonate a "lender" offering a great, guaranteed rate on a "pre-approved" loan. When a customer connects with the fraudster, the fraudster will emphasize that a poor credit history does not matter, and all the call recipient has to do to secure the pre-approved loan is pay a one-time fee up front.

16. These robocalls are often "spoofed" so that they falsely appear on a victim's caller ID to originate from U.S. federal government agency phone numbers, such as the SSA's main customer service number, local police departments, 911, or the actual customer service phone numbers of legitimate U.S. businesses. These "spoofed" numbers are used to disguise the origin of the robocalls and the caller's identities, and to cloak them with the authority of government agencies or large businesses to induce potential victims to answer or return the calls. In reality, the calls originate from fraudsters operating abroad, and have no connection to any U.S. government agency or other legitimate enterprise.

17. Individuals who answer or return these calls eventually speak to live fraudsters who tell the individuals lies intended to frighten and confuse them so that the fraudsters may begin to control their behavior and isolate them from authorities, friends, and family members. These lies often include that the individual's social security number or other personal

information has been implicated in criminal activity, that the individual faces imminent arrest or deportation, and that the individual's assets are about to be forfeited to the government. Once an individual is overcome by fear and panic, the fraudsters keep them on the phone and offer reassurances that the individual's purported legal problems can be resolved through payment of money, or that the individual's money must be transferred to the government agency the fraudsters are impersonating. The fraudsters often claim that the victim's payment will be returned in the immediate future. In reality, once the fraudsters are convinced they have extorted as much money as possible from the victim, they drop all contact, leaving the victim without meaningful recourse. Fraudsters receive victims' money through retail gift cards, bank wires, cash payments, cryptocurrency transfers, and other methods.

18. Since October 2018, the most prolific robocalling scam impersonating U.S. government officials—and one engaged in by Defendants—is impersonation of the SSA. For example, a robocall sent to millions of phones in the United States in early 2019 contained the following message:

> Hello this call is from Department of Social Security Administration the reason you have received this phone call from our department is to inform you that there is a legal enforcement actions filed on your social security number for fraudulent activities so when you get this message kindly call back at the earliest possible on our number before we begin with the legal proceedings that is 619-XXX-XXXX I repeat 619-XXX-XXXX thank you.

19. SSA received more than 465,000 complaints about fraudulent telephone impersonation of the Administration from October 1, 2018 through September 30, 2019. Losses associated with these complaints exceed $14 million. Similarly, the Federal Trade Commission ("FTC") reported that during 2018, its Consumer Sentinel database received more than 39,000 fraud complaints about SSA imposters, with estimated victim losses of approximately $11.5 million; for 2019, the FTC reported that SSA imposter call complaints rose to approximately

166,000 with associated losses of more than $37 million.[6] Complaint numbers substantially underrepresent the extent of the problem, because most victims do not report their losses to the government.

**B. How Calls From Foreign Fraudsters Reach U.S. Telephones**

20. The Defendants' robocalling fraud schemes, which involve robocalls that originate abroad and target individuals in the United States, are all dependent on VoIP and related technology to create the calls. VoIP calls use a broadband Internet connection – as opposed to an analog phone line – to place telephone calls locally, long distance, and internationally, without regard to whether the call recipient uses a cellular phone or a traditional, wired phone. The robocalling fraud schemes also require U.S. based telecommunications companies – referred to as "gateway carriers" – to introduce the foreign phone traffic into the U.S. phone system. A foreign call center or telecommunications company that places VoIP calls to U.S. telephones must have a relationship with a U.S. gateway carrier. From the gateway carrier, most VoIP calls will pass through a series of U.S.-based VoIP carriers before reaching a consumer-facing "common carrier" such as AT&T or Verizon, and ultimately a potential victim's phone. One of the Defendants' roles in the fraudulent schemes is to serve as a gateway carrier for the fraudulent robocalls.

21. Each provider in the chain that transmits a VoIP call maintains records, primarily for billing reasons, of all of the calls that pass through it. These records include the following information: the date and time of the call, the destination number (intended recipient), the source

[6] Regarding government imposter fraud more broadly and not limited just to SSA imposters, the FTC's Consumer Sentinel database contains 255,223 complaints reflecting $128,479,054 in losses for 2018, and 389,563 complaints reflecting $152,946,623 in losses for 2019.

number from which the call was placed (sometimes a real number and sometimes a spoofed number), the name of the company that sent the call to the provider, and the downstream company to which the provider sent the call. These records are generated automatically as a call is routed through telecommunications infrastructure in a manner that achieves the lowest cost to transmit a given call, known in the industry as "least-cost routing." Calls may be traced through these records back to their gateway carrier, and thus to their foreign source. The telecommunications industry refers to this process as "traceback."

22. Tracebacks of many different robocalling fraud schemes have led to the identification of Defendants as a gateway carrier willing to transmit huge volumes of fraudulent robocalls into the country, despite clear indicia of fraud in the call traffic and actual notice of fraud.

## DEFENDANTS' ONGOING PARTICIPATION IN ROBOCALLING FRAUD SCHEMES

23. Since at least 2016, and continuing through the present, Defendants have knowingly provided U.S.-bound calling services to foreign fraudsters operating robocall scams, acting as a gateway carrier and passing robocalls into the U.S. telephone system by the millions. The Defendants are paid for each call they pass into and through the U.S. phone system. In addition, the Defendants have provided return-calling services to the fraudsters operating the robocall scams, for which Defendants are also paid, enabling fraudsters to establish contact with unwitting individuals after the individuals are deceived by a robocall.

24. There is substantial evidence of the Defendants' knowledge of the fraudulent nature of the calls they transmit, including call records showing high percentages of short-

duration, unanswered calls[7] passing through their systems by the millions; thousands of spoofed calls originating from overseas, purporting to be from "911" and similar numbers; dozens of complaints and warnings from other telecommunications companies about fraud, spoofing, and short-duration "junk" calls; repeated warnings and inquiries from a telecommunications industry trade group about the fraudulent robocalls passing through the Defendants' system; and receipt of payment from their foreign customers in the form of large, suspicious cash deposits by various individuals throughout the United States directly into Defendants' bank accounts.

### A. Defendants Knowingly Introduce Fraudulent Robocalls into the U.S. Telephone System

25. Defendants provide inbound VoIP calling to the United States telecommunication system (referred to in the industry as "U.S. call termination") to customers located both here in the United States and abroad. Defendants provide unrestricted VoIP calling, meaning they do not monitor or restrict the inbound calls a customer can place for either volume of calls or call duration. Defendants are paid for each call they pass into and through the U.S. phone system.

26. Defendants specifically market their services to foreign call centers and foreign VoIP carriers looking to transmit high volumes of robocalls to individuals in the United States. The TollFreeDeals website states "TollFreeDeals.com is your premier connection for call center and dialer termination. We are always looking for the best call center routes in the telecom industry. We specialize in short call duration traffic or call center traffic. We understand there is a need for it and we want to help you find all the channels you need!"

[7] Short-duration and unanswered calls include calls where recipients immediately hang up and calls that do not connect, because robocalls are sent to numerous telephone numbers that are not in service.

27. The FAQs on the TollFreeDeals website state, "Do you handle CC (Call Center)/Dialer Traffic? Yes – unlike many carriers we will handle your dialer and call center VoIP termination minutes. If you are looking for USA Dialer, Canada Dialer, or Australia Dialer please fill out our online interop form to test our routes."

28. Defendants regularly transmit massive volumes of short duration calls. For example, over 23 days in May and June of 2019, TollFreeDeals transmitted more than *720 million* calls. Of those calls, more than 425 million, or 59% of the total calls, lasted less than one second in duration. In the telecommunications industry, high volumes of short-duration and unanswered calls are indicative of robocalls that are unwanted by the recipients, often because they are fraudulent. More than 24 million of those calls were placed to phone numbers with area codes in the Eastern District of New York. As Defendants' phone records show the ultimate destination number of every VoIP call they transmit, Defendants know they transmit fraudulent calls to potential victims in the Eastern District of New York.

29. During May and June of 2019, the Palumbos facilitated the delivery of more than 182 million calls through TollFreeDeals from a single India-based VoIP carrier co-conspirator to phones in the United States. One thousand different source numbers (the number from which a call is placed, and that shows up on the recipient's caller ID) accounted for more than 90% of those calls. According to data obtained from a robocall blocking company about calls identified as fraudulent robocalls in 2019, 79% of those 1000 source numbers have been identified as sending fraudulent robocalls. Consequently, TollFreeDeals transmitted an estimated 143 million fraudulent robocalls on behalf of that single India-based co-conspirator during May and June of 2019. Of those calls, an estimated 20% were Social Security imposter calls, 35% were loan

approval scams, and 14% were Microsoft refund scams. The remaining calls were a mixture of IRS imposter, U.S. Treasury imposter, miscellaneous tech support imposter and other schemes.

30. Defendants' knowledge of the fraudulent nature of the telephone calls they deliver to potential victims on behalf of their co-conspirators is also evidenced by the numerous complaints, inquiries, and warnings regarding fraudulent robocalls that Defendants received from other telecommunications carriers and a telecommunications industry trade association since at least 2017. Despite receiving these complaints, inquiries, and warnings, Defendants nevertheless continued to transmit massive volumes of fraudulent robocalls from their co-conspirators to potential victims in the United States.

31. For example, in May 2017, AT&T notified Nicholas Palumbo that it had traced back to TollFreeDeals robocalls received by its customers that spoofed phone numbers belonging to USCIS and the Office of the Inspector General of the U.S. Department of Homeland Security ("DHS-OIG"). AT&T informed Nicholas Palumbo that the callers who spoke to AT&T's customers impersonated U.S. Immigration Officers, and that AT&T had confirmed with USCIS and DHS-OIG that those agencies did not use any of the phone numbers at issue as a legitimate outbound caller ID. Nicholas Palumbo responded that the calls were transmitted to TollFreeDeals from an India-based VoIP carrier, and that he had blocked those two specific phone numbers. Blocking specific numbers is an ineffective means to stop fraudsters who are willing and have the ability to spoof any number as the caller ID number for their fraud calls.

32. In February 2019, AT&T notified Nicholas Palumbo that it had traced back 19 separate calls to AT&T customers that spoofed a USCIS phone number in order to "extort money from our customers." In Nicholas Palumbo's response to AT&T, he acknowledged that those calls were transmitted to TollFreeDeals from the same India-based VoIP carrier that had

transmitted spoofed USCIS calls in 2017. Despite repeated warnings from AT&T that this foreign VoIP carrier was transmitting fraudulent government-impersonation robocalls, the Palumbos continued transmitting VoIP calls on behalf of this customer through at least as recently as June 2019.

33. The Palumbos have also received numerous warnings from telecommunications industry trade association USTelecom that both TollFreeDeals.com and SIP Retail have transmitted fraudulent robocalls, including government impersonation robocalls.

34. From May 2019 through January 2020, TollFreeDeals received 144 notifications from USTelecom that a fraudulent robocall had been traced back to TollFreeDeals. Of these notifications, 83 referenced SSA imposter fraud calls, 24 referenced Tech Support imposter fraud calls, ten referenced IRS imposter fraud calls, and one referenced USCIS impersonation fraud calls. Each of these emails were sent to Nicholas Palumbo at his @tollfreedeals.com email address. Each email stated that a suspicious call had been traced back to TollFreeDeals's network and provided the call date, time and the source and destination phone numbers, to allow TollFreeDeals to identify the specific call at issue in its call logs (referred to in the industry as "call detail records"). Each email also provided a link to USTelecom's web-based traceback portal, where further information was provided about the specific fraudulent call at issue, included a recording of the fraudulent voicemail message that was sent to the recipient's phone. In every case, either the email itself or the traceback portal included a short description of the type of fraud at issue and the details of the fraudulent robocall campaign, such as:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million

per day. Because Caller-ID changes with each call, blocking the ANI ["Automatic Number Identification"[8]] is not effective.

35. After receiving each of these notifications from USTelecom, Nicholas Palumbo logged into the USTelecom portal and provided information regarding the customers of TollFreeDeals that had transmitted the fraudulent calls. Many of these fraudulent calls repeatedly traced back to the same India-based customers of TollFreeDeals.

36. From August 2019 through January 2020, USTelecom also notified SIP Retail of 35 tracebacks of fraudulent robocalls, including 19 tracebacks of SSA impersonation fraud calls, three tracebacks of Tech Support impersonation fraud calls, and one traceback of USCIS Impersonation fraud calls. Those notifications were emailed to help@sipretail.com. Upon information and belief, the Palumbos are the only individuals who monitor email traffic to @sipretail.com domain email addresses. SIP Retail logged into the USTelecom traceback portal and notified USTelecom that all 10 of the SSA impersonation calls were sent to SIP Retail by two India-based companies. Both of these companies were also sending fraudulent SSA imposter call traffic through TollFreeDeals.com, as the Palumbos have been notified by USTelecom on multiple occasions.

37. Further, Defendants regularly receive payment from their customers in the form of substantial cash deposits directly into Ecommerce's bank account, from locations throughout the United States raising red flags about the nature of the business of Defendants' customers.

**B. Defendants Provide Toll-Free Services for Robocall Schemes**

38. Not only do Defendants knowingly pass fraudulent robocalls by the millions into the U.S. telephone system, but they also provide return-calling services to fraudsters so that

[8] ANI refers to the origination telephone number from which a call is placed.

potential victims can call them back. These toll-free telephone numbers and related services are provided in the robocall message as call-back numbers, and appear to be U.S. telephone numbers and thus enable fraudsters to further deceive individuals about the robocall's origin and the identities and locations of the fraudsters at the other end of the call. In reality, what appears to the individual to be a U.S. telephone number is just a telephone number that Defendants register to an internet address designated by the fraudsters. Thus, the toll-free numbers can be used to ring telephones anywhere in the world.

39. While toll-free numbers used for return-calling purposes cannot be "spoofed" like outgoing robocalls, the use of a U.S. toll-free number in Defendants' robocalls schemes serves much the same purpose as spoofing—deception. The toll-free services provided by Defendants use VoIP technology to direct potential victims' return calls from the United States to the foreign fraudsters' call centers. The Defendants have knowingly provided toll-free numbers and associated calling services to foreign robocall fraudsters.

40. All toll-free numbers in the United States are administered by Somos, Inc., a company designated by the Federal Communications Commission ("FCC") as the national administrator of the U.S. toll-free calling system and its database. Among other functions within the industry, Somos registers "Responsible Organizations," that are authorized to provide toll-free numbers to their customers and to register those numbers in the national registry that the industry uses to direct toll-free telephone traffic. Defendants obtain toll-free numbers on behalf of their customers from one or more Responsible Organizations.

41. On July 31, 2019, an employee of a Responsible Organization sent the message below to Nicholas Palumbo via his @tollfreedeals.com email address:

Hello,

> We received a call yesterday (at 6 pm) that we didn't answer.
> Calling Number: +844[XXXXXXX]
> Requesting to call back: 844-[XXX]-[XXXX]
>
> Please see the attached audio and screenshot of the voicemail transcript. Shut down this user immediately as it was associated with the customer account of [TollFreeDeals customer]. These types of scam calls are prohibited from our network and further fraudulent calls from the same customer account will result in termination of said customer account. The number of 844-[XXX]-[XXXX] has been removed from your account in order to protect the integrity of our network.

The attached audio file of a voicemail message stated:

> tomorrow $399.99 is going to be deducted from your account for the remainder of your computer services. If you want to cancel the subscription, please press 1 to talk to our cancellation officer. Or you can call us back on our help line number 1-844-[XXX]-[XXXX]. I'll repeat the help line number 1-844-[XXX]-[XXXX]. Thank you."

42. Over the course of the next two weeks, employees of the Responsible Organization sent an additional six emails to Nicholas Palumbo, notifying him that the Responsible Organization was removing eight additional toll-free numbers from the accounts of two TollFreeDeals customers, because those numbers had been shown to be used in Tech Support impersonation scams and scams impersonating Amazon customer service. In response to each email, Nicholas Palumbo responded simply that he had let the customer of TollFreeDeals know.

43. On August 12, 2019, an employee of the Responsible Organization emailed Nicholas Palumbo and stated:

> Good afternoon Nick,
>
> I wanted to reach out to inform you that we have disabled the account of [TollFreeDeals customer] due to fraudulent complaints. Unfortunately, we do get a lot of complaints about customers under your reseller account. Our first line of defense when issues like arise we deactivate the customer's account. I am informing you that if we do receive any additional complaints about any of your other customers under your re-seller account, we will be forced to deactivate your account.

Nicholas Palumbo responded "I let him know," then responded further, "I will be porting clients over[.] Can't take that chance." In the telecommunications industry, to "port a number" means to move an existing phone number from one provider to another. In effect, Nicholas Palumbo was stating that he planned to take the toll-free numbers registered to his customers through the Responsible Organization who had warned him about fraudulent calls, and move those same numbers to another provider on behalf of his customers.

## HARM TO VICTIMS

44. Defendants' fraudulent schemes have caused substantial harm to numerous victims throughout the United States, including many victims located in the Eastern District of New York. It is estimated that Defendants and their foreign co-conspirators defrauded victims out of millions of dollars per year through fraudulent robocalls and return-calling services. If allowed to continue, these losses will continue to rise and result in further harm to victims.

45. In addition to the massive cumulative effect of these fraud schemes on victims throughout the United States, the harm can be devastating to individual victims. Victims have faced terrifying threats from fraudsters impersonating government officials and have lost substantial sums of money.

46. Defendants' fraudulent schemes are ongoing and wide-ranging. Absent injunctive relief by this Court, the Defendants will continue to cause injury to victims in this District and throughout the United States, and the victims' losses will continue to mount.

## COUNT I

(18 U.S.C. § 1345 – Injunctive Relief)

47. The United States realleges and incorporates by reference paragraphs 1 through 46 of this Complaint as though fully set forth herein.

48. By reason of the conduct described herein, Defendants violated, are violating, and are about to violate 18 U.S.C. §§ 1343 and 1349 by executing or conspiring to execute schemes or artifices to defraud, or for obtaining money or property by means of false or fraudulent pretenses with the intent to defraud, and in so doing, transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, writings, signs, signals, pictures, or sounds for the purpose of executing such schemes or artifices.

49. Upon a showing that Defendants are committing or about to commit wire fraud, conspiracy to commit wire fraud, or both, the United States is entitled, under 18 U.S.C. § 1345, to a temporary restraining order, a preliminary injunction, and a permanent injunction restraining all future fraudulent conduct and any other action that this Court deems just in order to prevent a continuing and substantial injury to the victims of fraud.

50. As a result of the foregoing, Defendants' conduct should be enjoined pursuant to 18 U.S.C. § 1345.

## PRAYER FOR RELIEF

WHEREFORE, the plaintiff United States of America requests of the Court the following relief:

A. That the Court issue an order, pursuant to 18 U.S.C. § 1345, pending a hearing and determination on the United States' application for a preliminary injunction, that Defendants, their agents, officers and employees, and all other persons and entities in active concert or participation with them are temporarily restrained from:

i. committing and conspiring to commit wire fraud, as defined by 18 U.S.C. §§ 1343 and 1349;

ii. providing, or causing others to provide call termination services for calls terminating in the United States or carrying any VoIP calls terminating in the United States;

iii. providing toll-free telephone services for calls originating in the United States, including providing toll-free phone numbers to other individuals or entities;

iv. destroying, deleting, removing, or transferring any and all business, financial, accounting, call detail, and other records concerning Defendants' operations and the operations of any other corporate entity owned or controlled, in whole or in part, by Defendants.

B. That the Court further order, pursuant to 18 U.S.C. § 1345, that within two days from Defendants' receipt of this Temporary Restraining Order and Order to Show Cause, Defendants shall provide copies of this Temporary Restraining Order and Order to Show Cause to all of their customers for whom they provide (1) United States call termination services, (2) United States toll-free call origination services; and to all entities (a) with whom Defendants have a contractual relationship for automated or least-cost call routing, or (b) from whom Defendants acquire toll-free numbers. Within four days from Defendants' receipt of the Temporary Restraining Order and Order to Show Cause, Defendants shall provide proof of such notice to the Court and the United States, including the names and addresses or email addresses of the entities and/or individuals to whom the notice was sent, how the notice was sent, and when the notice was sent.

C. That the Court further order, pursuant to 18 U.S.C. § 1345, Somos, Inc., in its capacity as the entity designated by the Federal Communications Commission to administer the U.S. toll-free calling system and its database, to temporarily suspend all toll-free numbers registered by or on behalf of any Defendant in this matter, until further order of this Court.

D. That the Court further order, pursuant to 18 U.S.C. § 1345, that any Toll-Free Service Provider that receives notice of this Temporary Restraining Order and Order to Show Cause and has a contractual relationship with one of the Defendants in this matter to provide toll-free numbers, shall provide to Somos, Inc. a list of all toll-free numbers provided to that Defendant that are currently active.

E. That the Court further order, pursuant to 18 U.S.C. § 1345, that any individual or entity who has obtained a toll-free number through one of the Defendants in this matter, either directly or through another intermediate entity, and wishes to continue using that toll-free number may submit a request to the Court, copying counsel for the United States, and identifying: (1) the individual or entity's name, address, phone number, email address, website URL, and the nature of their business; (2) the end-user of the toll-free number's name, address, phone number, email address, and website URL if the end-user did not obtain the toll-free number directly from Defendants; (3) the nature of the end-user's business; (4) the purpose for which the end-user utilizes the toll-free number; (5) the date on which the individual or entity obtained the toll-free number and, if applicable, provided it to the end-user; and (6) whether the toll-free number is used by the individual, entity, or end-user in connection with robocalls. The United States shall then notify the Court within four

business days whether the United States has any objection to removing the specifically identified toll-free number from the list of suspended numbers.

F. That the Court issue a preliminary injunction on the same basis and to the same effect.

G. That the Court issue a permanent injunction on the same basis and to the same effect.

H. That the Court order such other and further relief as the Court shall deem just and proper.

Dated: January 28, 2020

Respectfully submitted,

RICHARD P. DONOGHUE
United States Attorney

DARA OLDS
BONNI J. PERLIN
Assistant United States Attorneys
Eastern District of New York
271-A Cadman Plaza East
Brooklyn, New York 11201
Tel. (718) 254-7000
Fax: (718) 254-6081
dara.olds@usdoj.gov
bonni.perlin@usdoj.gov

JOSEPH H. HUNT
Assistant Attorney General
Civil Division
United States Department of Justice

DAVID M. MORRELL
Deputy Assistant Attorney General

GUSTAV W. EYLER
Director
Consumer Protection Branch

JILL P. FURMAN
Deputy Director

ANN F. ENTWISTLE
CHARLES B. DUNN
Trial Attorneys
U.S. Department of Justice
P.O. Box 386
Washington, D.C. 20044
Tel. (202) 307-0066
Tel. (202) 305-7227
Fax: (202) 514-88742
Ann. F. Entwistle@usdoj.gov
Charles.B.Dunn@usdoj.gov